Notice of Allowability	Application No.	Applicant(s)	
	09/390,362	VANSTONE ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *12/18/2006*.

2. ☒ The allowed claim(s) is/are *1-14*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

The prior election/restriction requirement is withdrawn due to applicant adding linking claim 14.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Ralph Dowell (Reg #: 26,868) on 3/8/2007. The amendments are to overcome minor objections to the claims. As per MPEP 713.04, because the substance of the interview has been included herein, a separate interview summary form is not provided.

The application has been amended as follows:

Claim 1 (currently amended) A method of digitally signing a plaintext message exchanged between a pair of correspondents in a data transmission system, one of said pair of correspondents being the signer and having a private key *a*, said public key being available to the other of said pair of correspondents, said method comprising the steps of:

subdividing said plaintext message into a first plaintext bit string H and a second plaintext bit string V;

computing a first signature component c as a function of said first plaintext bit string H wherein the plaintext bit string H is hidden in said first signature component c;

computing an intermediate signature component c' as a function of said first signature component c and said second plaintext bit string V;

computing a second signature component s as a function of said intermediate signature component c' and said private key *a*; and

forming a signature (s,c,V) containing said first signature component c, said second signature component s, and said second plaintext bit string V as discrete signature components;

wherein by during verification, said second plaintext bit string V is available from said signature (s,c,V) as an input to a verification protocol.

Claim 8 (currently amended) A method according to claim 7 wherein said combining ~~combination~~ of said first component and said second plaintext bit string V includes hashing ~~a combination of~~ said first component and said second plaintext bit string V.

Claim 14 (currently amended) A method for authenticating a communication between a first correspondent and a second correspondent in a data transmission system, said first correspondent having a private key *a* and a public key derived from the private key *a*, said public key being available to said second correspondent, said method comprising:

said first correspondent subdividing a plaintext message into a first plaintext bit string H and a second plaintext bit string V;

said first correspondent computing a first signature component c as a function of said first plaintext bits string H wherein the plaintext bit string is hidden in said first signature component c;

said first correspondent computing an intermediate signature component c' as a function of said first signature component c and said second plaintext bit string V;

said first correspondent computing a second signature component s as a function of said intermediate signature component c' and said private key a;

said first correspondent forming a signature (s,c,V) containing said first signature component c, said second component s, and said second plaintext bit string V as discrete signature components;

said first correspondent making available to said second correspondent, at least said first signature component c and said plaintext bit string V;

said second correspondent generating a value by combining said first signature component c with said second plaintext bit string V;

said second correspondent recovering said first plaintext bit string H from said value using publicly available information of said first correspondent including said public key;

said second correspondent examining said recovered first plaintext bit string H for a predetermined characteristic; and

said second correspondent verifying said message if said predetermined characteristic is present.

The following is an examiner's statement of reasons for allowance:

As per claim 1, the prior art does not teach the specific steps of signature generation as recited in the claim. The closest prior art were by McCollom (EP 0918274) and ISO/IEC 9796-2 used in the rejections in the prior office action before applicant amended the claims. The differences though is that the final signature in McCollum is not composed of three discrete signature components as recited in claim, whereby during verification, said second plaintext bit string V is available from the signature as input into a verification protocol. With ISO/IEC 9796-2, while teaching discrete signature components in the partial recovery scheme, the signature components were only comprised of two components. While the second component of ISO/IEC 9796-2's signature is similar to component V recited in the claim, the first component of ISO/IEC 9796-2's signature is different from both components s and c of claim 1. Further, the steps of forming components c' and s as recited in claim 1 were not taught by ISO/IEC 9796-2.

With respect to claim 7, ISO/IEC 9796-2 was the closest prior art to the recited limitations. However, ISO/IEC 9796-2 does not teach generating a value by combining said first component with said second plaintext bit string V; recovering said first plaintext bit string H from said value using publicly available information of the purported signer including said public key; examining said recovered first plaintext bit string H for a predetermined characteristic; and verifying said message if said predetermined characteristic is present. As can be seen in the appendix of ISO/IEC 9796-2, section

A.5, the second component of the plaintext message is not used at all in the signature verification function, while the verification in claim 7 utilizes the second component to do verification by first generating a value using the second component.

Claim 14 contains a combination of what is recited in claims 1 and 7 and is allowable for the same reasons 1 and 7 are allowable. The rest of the claims are allowable due to dependency on claims 1 and 7.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100